Attorney's Docket No.: SPAM/SCH

APPLICATION

FOR

UNITED STATES LETTERS PATENT

TITLE: AUTOMATIC MAIL REJECTION FEATURE

APPLICANT: SCOTT C. HARRIS

CERTIFICATE OF MAILING BY EXPRESS MAIL

Express Mail Label No. EM 327 460 746 US

This correspondence is being deposited with the United States Postal Service as Express Mail Post Office to Addressee with sufficient postage on the date indicated below and is addressed to the Assistant Commissioner for Patents, Washington, D.C. 20231.

October 16, 2000
Date of Deposit

Signature

Janet Christy
Typed or Printed Name of Person Signing Certificate

AUTOMATIC MAIL REJECTION FEATURE

This application claims priority from provisional application no 60/203,729, filed May 12, 2000.

Background

This invention relates to an automatic mail rejection feature in an e-mail program.

E-mail can be an inexpensive and effective way of sending information. Because of this, a recurrent problem is "spam", or the sending of unwanted email to a certain person. Once an e-mail address gets on a spammer's list, the person can be barraged with junk email. Various attempts have been made to combat this problem.

For example, some web e-mail programs include the ability to block further mail from a specified sender. When junk mail is received from a specified address, the control is actuated. Further mail from that specified sender is then blocked, presumably automatically deleted or sent to the trash.

Certain laws also cover spamming, and require that each e-mail that is sent unsolicited have a way of unsubscribing from the list. Spammers combat both of these measures by continually changing their name and/or changing their return address.

Some e-mail programs allow a user to manually set criteria for rejection of incoming email. For example, if an incoming e-mail is from a domain that has many known spammers, many people may simply set their program to delete it. However, this has the unintended extra effect of also removing desired email, at times.

In addition, the automatic rejection feature does nothing to resolve the traffic caused by junk e-mail.

Summary

The present application teaches an automatic system which automatically recognizes certain aspects of undesired messages such as junk email and undesired Internet content. The system automatically produces recommendations of criteria to use in automatically removing undesired information.

In an email embodiment described herein, these criteria can be automatically enforced or can be presented to the user as a table of options. In addition, the system can look for keywords in the e-mail, and can automatically postulate strategies for rules based on these keywords.

Brief Description of the Drawings

These and other aspects will be described in detail with reference to the accompanying drawings, wherein:

Figure 1 shows an email browser window;

Figure 2 shows a determined spam message, and the parsing scheme used on it;

Figure 3 shows an exemplary computer system; and

Figure 4 shows and operational flowchart.

Description of the Preferred Embodiment

A first embodiment describes an e-mail program which allows automatic rejection of unwanted messages. The embodiment runs on a computer shown in Figure 3, having a processor 300 and memory 305. A typical e-mail browser window is shown in Figure 1. The browser window include a number of operating buttons 102, a list of return addresses, and message subject. This browser also includes and displays a measure of likelihood of spam quotient or "LOSQ". The likelihood of spam quotient is displayed in the rightmost column as a percentage. For example, a message that is known to be spam would have a likelihood of spam quotient of 100%. Other messages that are less likely to be spam may have a likelihood of spam quotient of something less than 100%.

The likelihood of spam quotient can be displayed as a number as shown in Figure 1, or alternately can be displayed by the color of the message being displayed. For example, the message can be displayed in green to indicate low likelihood of spam (e.g. less than 10%) and yellow to indicate medium likelihood of spam (e.g. between 10 and 80 percent, and in red to indicate high likelihood of spam; for example likelihood of 80 to 100 percent to be spam, for example.

One of the buttons 106 on the toolbar requests removal of the high spam likelihood messages from the inbox. This enables, in a single click, removing all high likelihood of spam messages. Another button 120 is an options button which brings up the options menu of Figure 2.

The function buttons in Figure 1 include, as conventional, a delete message button 107. An additional a "delete as spam" button 111 is also provided. Any message that is deleted as being spam is further processed to determine characteristics that can be used to process other messages. Characteristics of the deleted-as-spam message are used to update the rules database to indicate characteristics of the spamming messages.

Another button 112 is also provided indicating "delete the message; not spam". Therefore, the user is presented with three different options: delete the message without indicating whether it is spam or not, delete the message while indicating that it is spam, or delete the message indicating that it is not spam.

The latter two options are used to update the rules in the rules database as described in further detail herein. Hence, this option allows adding an incoming e-mail message to the spam list, when it is determined to be likely to be spam.

Figure 1 also shows a number of different ways of displaying different email. The first option, labeled "show all messages", on button 104, has the function, as it suggests, of showing all messages. The messages may be further characterized based on the likelihood that they are spam. As described herein, the messages are characterized by comparing them with rules. Each match with the rules may increase the score, and make it more likely that the message is spam. More about this operation is described herein.

Those messages which are likely not spam are shown in a neutral color such as green or black. The messages which are questionable are shown in a cautionary color, such as yellow highlight. Finally, the messages which are likely to be spam are shown in an alert color such as red.

A second display option displays only those messages which are likely to represent desired messages. Hence, only the green and yellow messages are displayed. According to one embodiment, the messages are sorted by date and time received. Within each day, the messages are sorted by likelihood of being spam. The spam-likely messages, which are determined to be likely to represent spam, may be put into a separate folder; here shown as "spam-likely messages".

The messages which are likely to represent undesired information can be read by the user. If not read by the user, they are kept in the folder for a specified period of time e.g. thirty days, before deleting.

The incoming messages are processed based on rules. For example, if one does not want to be on a mailing list about XXX type items, then messages that include the text "free xxx pictures" may be likely to be spam. However, other people may find those messages to be highly desirable. Similarly, messages about get rich quick schemes may be trash to one person, treasure to another.

The present system allows customization of which emails to remove as spam, by defining rules. Each time a message is deleted as spam, a number of aspects about that message are stored. A database is used to store the message. This database may include relative weighting of different aspects. Figure 2 shows a determined spam message, and the parsing scheme.

The sender of the message is often a highly determinative factor. For example, if a specific sender sends one spam message, the same sender is very likely to be sending another spam message later on. Therefore, a first item in the database is the "received from" field 202. In addition to the specific sender, however, the domain of the sender often gives information. This domain is reviewed at 204. If the domain is a common domain such as Yahoo.com or Hotmail.com, then the relevance of the sender's domain may not be probative. If, however, the domain name is uncommon, such getrichquick.com or the like, then it is more likely that other message from that domain would be spam. Further, many messages from a common domain may itself be probative. The domain information is weighted accordingly.

The domain name from an item is added to the rules database from field 204. Another field 206 stores an indication of whether the domain is a common domain or an uncommon/ specific domain. This determination is initially zero, and is changed depending on the number of hits of domains that become present in the database. For example, when two different addresses from the same domain become spam, then the value becomes presumptly H (likely to be spam). When two different addresses from the same domain are received, one spam, the other not, then the value presumptively becomes L.

Each sentence and field in the e-mail, including subject; text of the body; links in the email, and any others is then stored as a separate field.

Analogous information may also be categorized from emails that are deleted as "not spam". This provides a database of characteristics that are likely to represent spam messages, and other characteristics that are less likely to represent spam messages. Matching with the databases changes the scoring of the message accordingly.

Once the database becomes sufficiently large, it may become time-consuming to compare incoming messages with the database. Indexing approaches can be used to increase the speed of the comparison. The detailed comparison may also be done in the background; the message may be displayed, and its classification displayed only some time later.

Figure 4 shows incoming messages received at 400 being broken down into analogous parts to those parts that are cataloged in the database 410. Each part in the incoming e-mail is compared with each part in the database. A simplified index can be prepared, such as the type used for internet searching, in order to speed up the searching. Each match changes the scoring of the email, to make it more likely to be spam, or less likely to be spam at 415. Each field match has a specified score increase. For example, match from the addressee is a very powerful indication of spam, and may by itself carry a score of 75. 100% matching of a sentence may carry a score of 10. A 50% word match may carry a score of 3. Match of the hyperlinks in an e-mail to those in a previously spammed determined e-mail may carry a score of 5.

Similarly, the e-mail and its fields can be compared with non-spam indicative email. An e-mail which is not spam can carry negative scores, for example. Finding the e-mail address to be on the non-spam list, for example, can carry a score of negative 100, or can immediately abort the process with an indication of non-spam.

If a message has few matches to the database, it may be characterized as unknown or cautionary (yellow). Similarly, mixed signals (some matches to spam and non-spam database), may result in an unknown result.

The total score for an e-mail is assessed, and this total score is used to assess if the e-mail is spam or not.

If the e-mail is determined to be spam, then it is appropriately processed.

Many different rules databases can be used. Such modifications are intended to be encompassed.